(12) UK Patent Application (19) GB (11) 2 314 436 (13) A

(43) Date of A Publication 24.12.1997

(21) Application No 9712528.0

(22) Date of Filing 17.06.1997

(30) Priority Data
(31) 08/664348 (32) 17.06.1996 (33) US

(51) INT CL[6]
G07F 19/00

(52) UK CL (Edition O)
G4H HTG H1A H13D H14A H14B H14D
U1S S2213

(56) Documents Cited
GB 2112190 A US 5365574 A US 5311594 A

(58) Field of Search
UK CL (Edition O) G4H HTG
INT CL[6] G07C , G07F

(71) Applicant(s)
Mitel Corporation

(Incorporated in Canada)

PO Box 13089, 350 Legget Drive, Kanata, Ontario, K2K 1X3, Canada

(72) Inventor(s)
Roland Michaud

(74) Agent and/or Address for Service
Dummett Copp
25 The Square, Martlesham Heath, IPSWICH, Suffolk, IP5 3SL, United Kingdom

(54) Customer authentication apparatus

(57) Customer authentication apparatus, e.g. for use over a telephone network, for authenticating a customer wishing to access a service, stores digital data in a memory 1, the digital data representing information associated with each customer, randomly generates a stimulus 2,108, related to the stored data and presents 5,101,102,103 the stimulus to a customer wishing to access the service, accepts customer input 5,101,102,103 in response to the stimulus and generates customer response data therefrom 107, compares the customer response data with the stored data 2,9, repeats the above steps on an iterative basis, and validates the customer when the customer response data match the stored data within predefined limits.

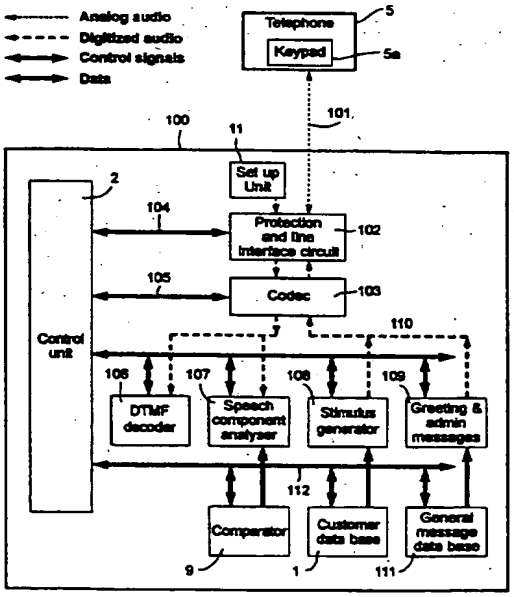

Fig. 1

GB 2 314 436 A

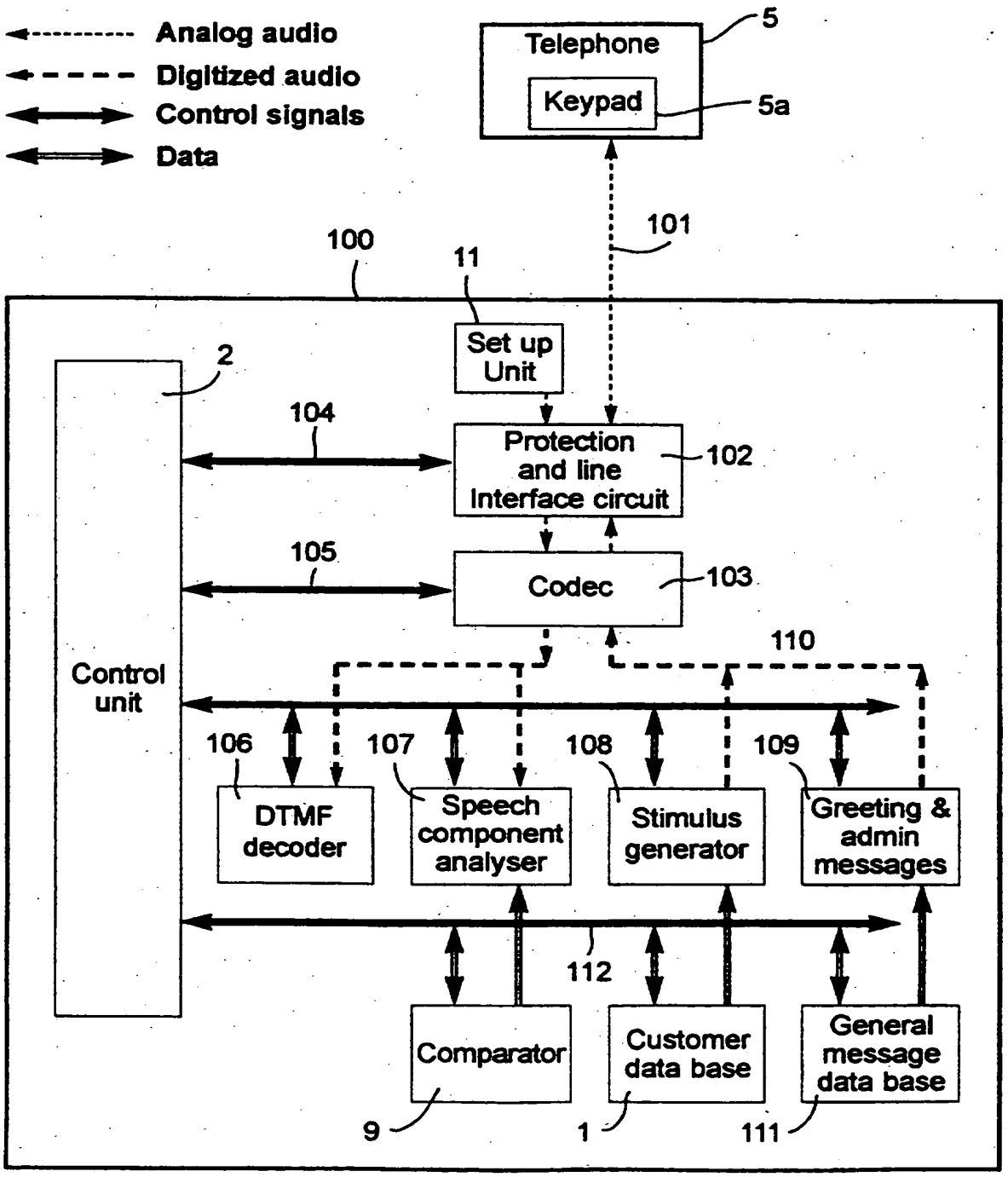
Analog audio
Digitized audio
Control signals
Data
Telephone
5
Keypad
5a
101
100
11
Set up Unit
2
104
Protection and line Interface circuit
102
105
Codec
103
110
Control unit
106
107
108
109
DTMF decoder
Speech component analyser
Stimulus generator
Greeting & admin messages
112
Comparator
Customer data base
General message data base
9
1
111

Fig. 1

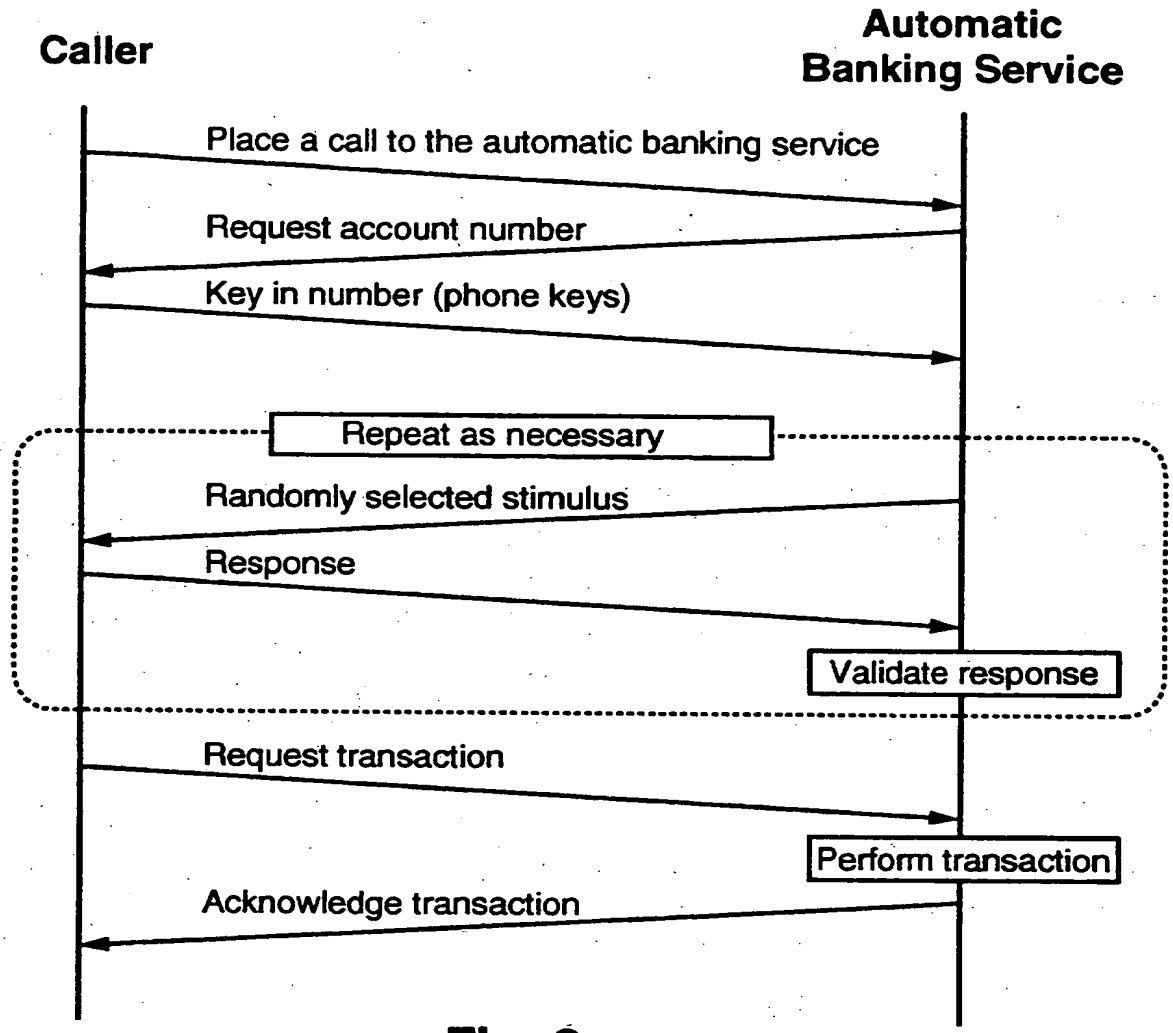
Caller
Automatic Banking Service
Place a call to the automatic banking service
Request account number
Key in number (phone keys)
Repeat as necessary
Randomly selected stimulus
Response
Validate response
Request transaction
Perform transaction
Acknowledge transaction

Fig. 2

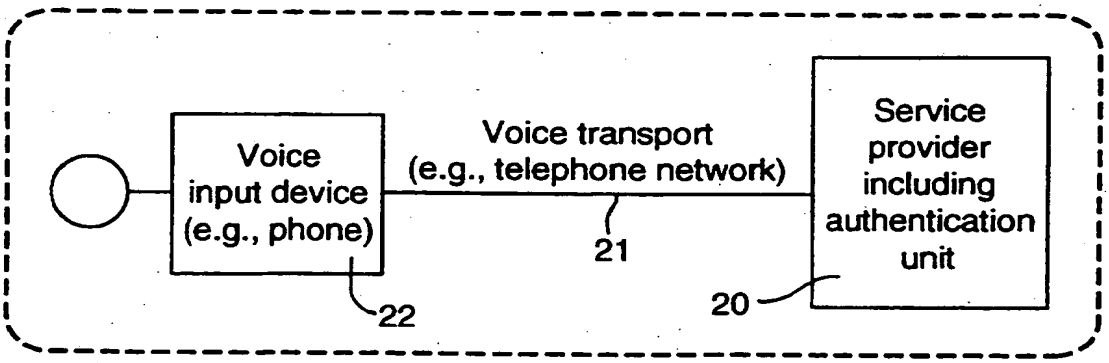
Voice input device (e.g., phone)
Voice transport (e.g., telephone network)
Service provider including authentication unit
21
22
20

Fig. 3

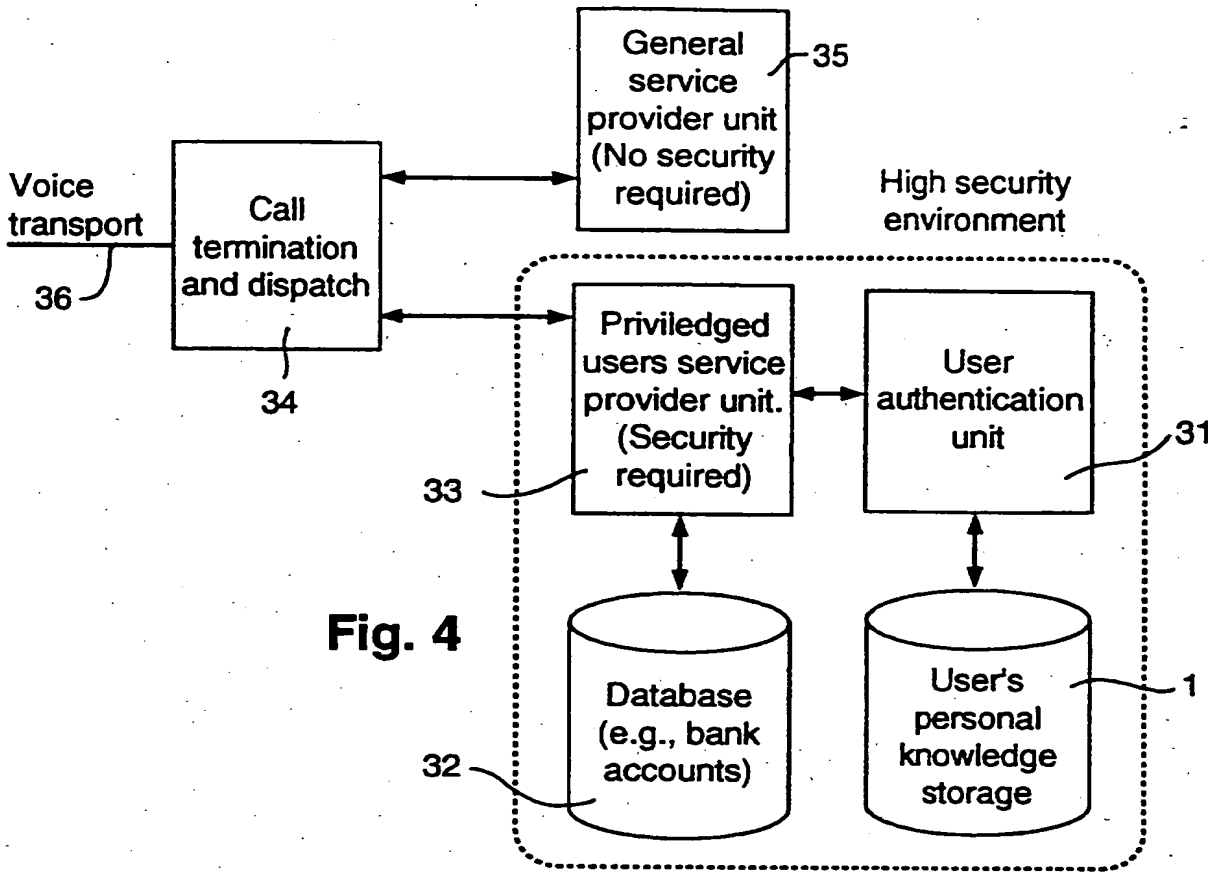
General service provider unit (No security required)
35
Voice transport
36
Call termination and dispatch
34
High security environment
Priviledged users service provider unit. (Security required)
33
User authentication unit
31
Database (e.g., bank accounts)
32
User's personal knowledge storage
1

Fig. 4

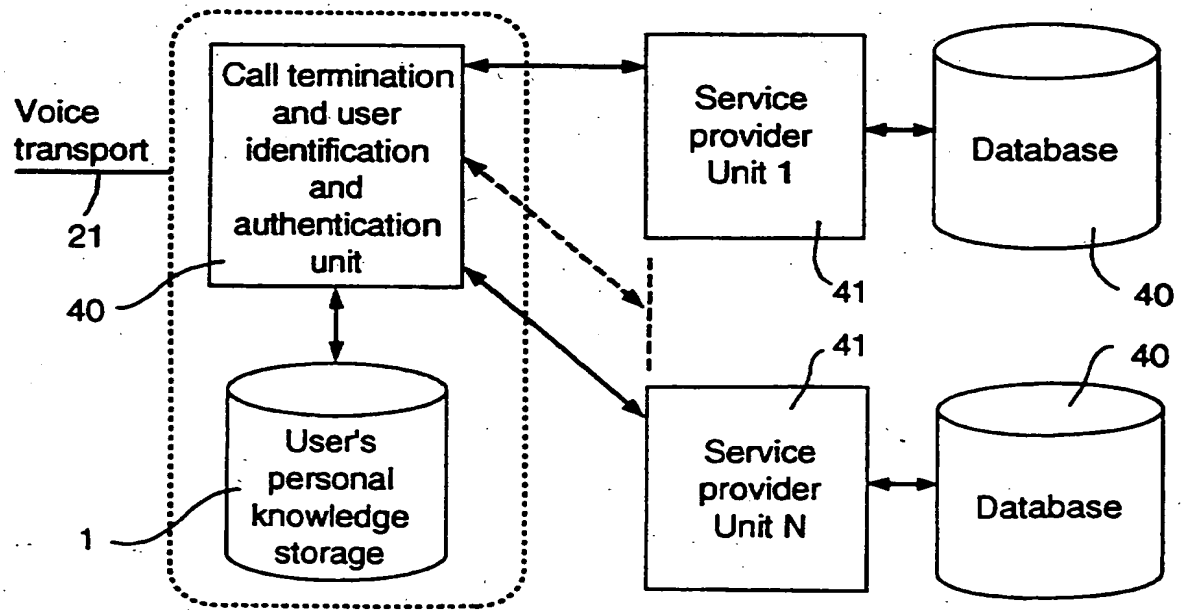
Voice transport
21
Call termination and user identification and authentication unit
40
User's personal knowledge storage
1
Service provider Unit 1
41
Database
40
Service provider Unit N
41
Database
40

Fig. 5

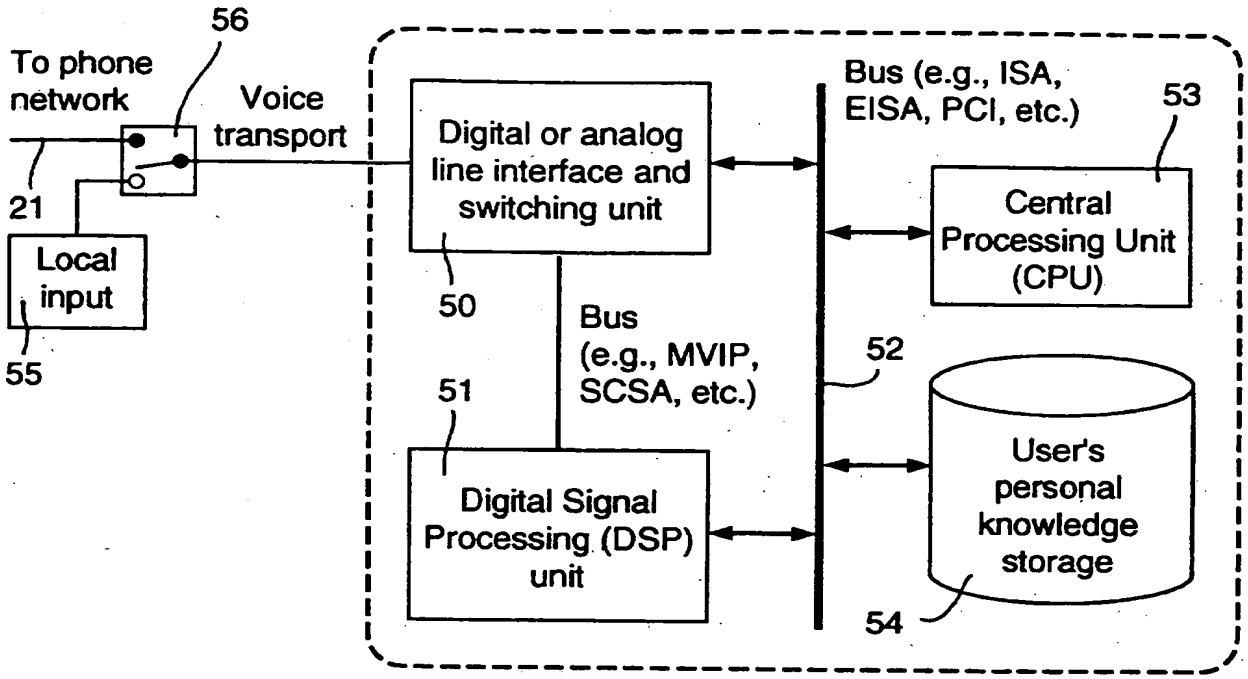
56
To phone network
Voice transport
21
Local input
55
Digital or analog line interface and switching unit
50
Bus (e.g., ISA, EISA, PCI, etc.)
53
Central Processing Unit (CPU)
Bus (e.g., MVIP, SCSA, etc.)
51
52
Digital Signal Processing (DSP) unit
User's personal knowledge storage
54

Fig. 6

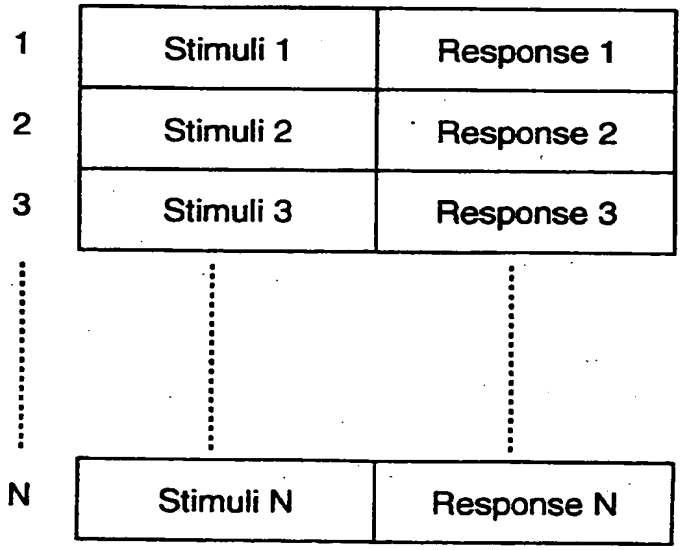
1
Stimuli 1
Response 1
2
Stimuli 2
Response 2
3
Stimuli 3
Response 3
N
Stimuli N
Response N

Fig. 7

CUSTOMER AUTHENTICATION APPARATUS

This invention relates to customer authentication apparatus, and more particularly to such apparatus for use over a telephone network, and to a method of authenticating a customer wishing to access a service.

In modern society, the telephone is being increasingly used as a means for a customer to obtain services without the need to travel. An impediment of the spread of such remote services is the risk of fraud due to inadequate customer authentication.

Credit card companies have long kept a file on personal data, such as a person's mother's maiden name, that is unlikely to be known by fraudulent users. If a customer wishes to obtain information about his or her account, the operator will ask questions drawn from the customer file. This system requires operator intervention and can be defeated by a determined fraudulent user who could obtain the limited number of items of information by carrying out the necessary research in advance. Such a system has not yet been applied to automated telephone services.

An object of the invention is to provide a secure customer authentication system suitable remote access of automated services.

Accordingly the present invention provides a method of authenticating a customer wishing to access a service, comprising the steps of storing digital data in a memory, the digital data representing information associated with each customer, randomly generating a stimulus related to the stored data and presenting said stimulus to a customer

wishing to access the service, accepting customer input in response to the stimulus and generating customer response data therefrom, comparing the customer response data with the stored data, repeating such steps on an iterative basis, and validating the customer when the customer response data match the stored data within predefined limits.

In a preferred embodiment, customer authentication is performed in two steps based on:

1) Customer voice print authentication; and
2) Customer personal knowledge verification.

Depending on the level of security required, one or both steps may be used.

In one embodiment, the customer is first asked to repeat a series of spoken words and these are matched with previous digitally stored recordings made by the customer to perform voice signature verification. The customer is then asked a series of questions, and his or her responses are first recognized using a voice recognition unit. They are then matched with knowledge items stored in the data base. Both the spoken words and the knowledge items are randomly selected as a subset of the set of records in the data base. The total number of records can be quite large so as to reduce the chances of a fraudulent user being able to obtain all the answers. Voice recognition can be performed on the responses or not at all.

The two checks can be combined in that, if desired, voice print authentication can be carried on the customer's responses to knowledge-based queries.

If desired, a timer can be arranged to time out if the user does not respond to a question within the predetermined period of time. An authentic customer will generally be able to respond to the questions immediately whereas the fraudulent user, given the large number of questions, might have to refer to a reference source, and the timer can limit the opportunity to do so by timing out if the response has not been given within a certain time period.

The invention is particularly adapted for telephone systems with a remote telephone providing the stimuli and accepting the customer input, and the remaining part of the equipment being at the service provider's premises.

One particular application of the invention is bank account manipulation. Once a person has been authenticated as a valid customer, he or she can then carry out bank transactions from any remote location (e.g. home) using the telephone key pad. The latter, if desired, can be used as a means of accepting customer input, although voice commands are preferred because they are faster.

The invention also provides customer authentication apparatus comprising a memory for storing digital data representing information items associated with each customer, a selection unit for randomly selecting digital data associated with an information item on an iterative basis, transducer means for presenting a stimulus related to the stored data to a customer wishing to access the service, input means for accepting customer input in response to the stimulus and generating customer response data therefrom, a comparator for comparing the customer

response data with the stored data and validation means for validating the customer when the customer response data match the stored data within predefined limits.

The transducer means and input means can conveniently be provided by a remote telephone.

The invention can require a perfect match to all responses, although this may be unrealistic. For example, people do not always pronounce words in exactly the same way and a legitimate customer might inadvertently give the wrong response to a question. The invention makes a decision on the basis of the number of correct and wrong answers. Criteria for determining validity can be set in advance. Furthermore, the number of iterations is flexible, and if the customer gives wrong answers or the equipment fails to recognize a voice response, the number of iterations can be increased so that the probability of error is small.

This invention thus allows a service provider to recognize and validate the identity of a caller by using two authentication mechanisms, either alone or in combination:

a) voice signature verification

b) caller personal knowledge verification

Task b is done by requesting verbal feedback from the caller using a randomly selected subset of stimuli based on a set of pre-recorded knowledge items. In summary, the authentication system can perform voice signature verification as well as user personal knowledge verification either concurrently or separately.

Voice signature may be performed on one or more pre-defined set of sounds (e.g., words). If technology permits a wide choice of words for signature verification, then, the request for the signature word(s) should consist of a subset of responses to a randomly selected set of stimuli. Voice recognition can be performed by an system that performs voice processing on sounds or phonemes. A suitable is VPRO by Voice Processing Corporation of Cambridge, Massachusetts, USA.

The service provider needs a database for each identity it needs to validate. This is done by recording a set of responses corresponding to a set of stimuli. During validation, only a subset of the stimuli will be picked randomly for validating the person's identity. The stimuli would typically (but not necessarily) be presented in the form of a question. The response should involve a limited set of syllables so as to facilitate the processing of the voice print.

The stimuli must call, not only on the person's knowledge but also on the language ability of the person. If a person is fluent, or has certain competence in more than one language, the stimuli should use the person's ability to understand stimuli in the languages he or she understands, and to provide the responses in these languages as well.

The personal stimuli database have to be created by deciding on a set of stimuli for which the person can easily remember the response. Ideal stimuli should appeal to knowledge acquired during user's childhood. For safety reasons, the stimuli should be spoken by a person other than the person which will use the validation system.

Then the answers/responses must be recorded as spoken by the target person. Obviously, all stimuli and responses have to be tested thoroughly.

The invention will now be described in more detail, by way of example only, with reference to the accompanying drawings in which:

Figure 1 is a block diagram of customer authentication apparatus in accordance with the invention;

Figure 2 illustrates a sample validation hand-shaking session;

Figure 3 illustrates a typical end-to-end operating environment;

Figure 4 shows the customer authentication apparatus as adjunct to a service provider;

Figure 5 shows a customer authentication apparatus as a front end to a service provider system;

Figure 6 shows a physical embodiment of a customer authentication apparatus; and

Figure 7 shows a database structure suitable for use in the customer authentication apparatus.

Referring now to Figure 1, an authentication apparatus 100 is connected to a telephone 5 with a keypad 5a over a telephone line 101, which is connected in the apparatus 100 to a protection and line interface circuit 102. This is in turn connected to a codec 103 for digitally encoding or decoding analogue signals arriving from or going to the telephone line 101. The codec 103 is also connected to the interface circuit 102 and a control unit 2, which also serves as a validation unit. Control signals pass between the control unit 2 and the circuits 102, 103 over lines 104, 105.

The codec 103 is connected to a DTMF decoder 106, a speech component analyzer 107, a stimulus generator 108, and a greeting and admin message generator 109. These units are all connected to the control unit 2 via line 110.

The speech component analyzer 107, stimulus generator 108, and greeting and admin message unit 109 are respectively connected to a comparator 9, customer database 1, and general message database 111. The latter units are connected to the control unit 2 by line 112.

Database 1 stores in digital form a large number of groups of data items, each group being associated with a particular customer. Some of the data items comprise digitized representations of the customer speaking selected words, and some represent responses to questions within the personal knowledge of the customer. The knowledge items could, for example, include the maiden name of the customer's mother, the names of any close relatives of the customer or any general knowledge of the customer, perhaps pertaining to the place where the customer was brought up or went to school. If the

customer is familiar with more than one language, knowledge items can be stored in any language familiar to the customer.

On initiation of a call, control unit 2 sends a message, which is the same for all customers, requesting the customer to enter his or her account number through the keypad. This is converted into an audio message in the codec 103. The customer keys in his or her account number through the telephone keypad 5a, and the response signals are decoded by DTMF decoder 106, which passes the results to the control unit 2.

The control unit 2 then randomly selects data items from the database 1 corresponding to the received account number, and passes these data items to the telephone 5 through the codec 103. The customer normally responds verbally although except in the case of mismatching data, the customer can also respond through the keypad using DTMF tones.

Assuming the customer responds verbally, the response data is passed through codec 103 to the comparator 9, which compares the response data with the corresponding stored data in the database 1. The control unit 2 then allocates a score to the correct responses and makes a decision according to predefined criteria. The control unit 2 can be designed to require all responses to be correct, although it can allow for some errors depending on the design of the system and the level of security required.

The speech component analyzer 107 checks the voice-print of the customer. This can be in response to a request for

the customer to pronounce certain words stored in the customer database, and/or the answers supplied to the knowledge-based queries. For example, if the system asks for the customer's mother's maiden name, the control unit can verify both that the answer is factually correct and that the answer matches the customer's voice-print. This can be done either by using voice-print analysis techniques or by storing a digital representation of the customer actually responding to the question.

Figure 2 illustrates a typical banking transaction using apparatus in accordance with the invention. The caller is identified on the left hand side of the figure and the automatic banking service on the right. First the caller places a call to the automatic banking service, which in turn responds by requesting the account number, which the caller enters by using the telephone keypad. The account number is transmitted as DTMF tones (although dial pulses can be used) to the automatic banking service which then initiates operation of the customer authentication cycle.

A random stimulus is selected from the database 1, and the customer's response validated. If the response is valid, the cycle is repeated with a different randomly selected stimulus. If his response is incorrect, the system can either repeat the stimulus or note the response as incorrect and move onto the next stimulus. In either case, the control unit 2 notes the incorrect response.

After a certain number of iterations, the customer is deemed authentic, and the system notifies the customer that he has been authenticated and that he can request a transaction. The customer then requests the transaction, which is carried out by the automatic banking service.

After the transaction has been carried out, the automatic banking service sends an acknowledgment to the customer who can then hang up or request another transaction.

Figure 3 shows a more generic illustration of the invention. In Figure 3 a service provider 20 includes an authentication apparatus in accordance with the invention. The service provider communicates over any voice transport system 21, for example a telephone network, to a voice input device 22, which could be a telephone.

Figure 4 shows a customer authentication apparatus in accordance with the invention as an adjunct to a service provider. Service provider 30 includes an authentication unit 31 connected to customer database 1. The service provider database 32 contains information that customers desire to access and manipulate. For instance, database 32 may contain bank accounts and the like. Interaction with the service provider 30 is through the privileged user's unit 33 which is connected to the authentication unit 31. The privileged user's unit communicates with a call termination and dispatch unit 34 connected to the telephone line 36. The latter unit is also connected to a general service provider unit 35, which does not require security.

Figure 5 shows another configuration of the invention where the authentication unit is provided as a front end to a multiple service provider system. Telephone line 21 is connected to call termination and user identification and authentication unit 40 connected to user's personal knowledge database 1. A calling customer is authenticated in the manner described with reference to Figure 2. Once authenticated, the customer can be connected to any one of

the desired service providers 41 each connected to associated database units 40 containing information desired to be accessed or manipulated by the customer.

Figure 6 shows the physical embodiment of an authentication unit in accordance with the invention. Telephone line 21 is connected to digital or analogue interface and switching unit 50 through switch 56. The latter allows the unit 50 to be alternatively connected to a local input 55 for set-up mode or control purposes. Unit 50 is connected over bus, for example an MVIP or SCSA bus to a digital signal processing unit 51. Interface unit 50 and DSP unit 51 are connected to another bus 52, which could be an ISA bus, or an EISA bus, for example. Central processing unit 53 and user's personal knowledge storage database 54 are connected to the bus 52. The implementation shown in Figure 6 is a more practical implementation than the one shown in Figure 1, which helps understand the principles of the invention, since it uses modern digital signal processing and bus technology.

In Figure 6, the interface for the voice media connects the voice circuit to the DSP unit when required for voice signature analysis and stimulus-response handshake. A high speed connection is provided between these two resources, and this can be implemented using the disclosed MVIP or SCSA bus.

Figure 7 shows the functional organization of the personal knowledge database 1. Each stimulus S_N is associated with a corresponding response R_N. The stimulus could be for example a request to speak a word in which case the stored response is a digitized representation of the customer previously speaking the word. If the stimulus is a

question, then the response is the expected answer.

For each new customer, the personal database must of course be established. This can achieved by the customer visiting the service provider premises and providing a series of responses through set-up unit 11 (see Figure 1), which can, for example, include a telephone handset. The control unit 2 simply requests the new customer to provide answers to a wide range of question and repeat certain selected words. The responses are digitized and stored in the new customer's personal information database within the database 1.

It will be observed that the invention thus provides an authentication method and apparatus that offers secure customer validation in a telephone environment. It will be obvious that the skilled person in the art will be able to devise many different means of implementing the invention without departing from the scope of the invention as defined in the claims.

Claims:

1. A method of authenticating a customer wishing to access a service, characterized in that it comprises the steps of:

a) storing digital data in a memory, said digital data representing information associated with each customer;

b) randomly generating a stimulus related to said stored data and presenting said stimulus to a customer wishing to access the service;

c) accepting customer input in response to said stimulus and generating customer response data therefrom;

d) comparing said customer response data with said stored data;

e) repeating steps b to d on an iterative basis; and

f) validating said customer when said customer response data match said stored data within predefined limits.

2. A method as claimed in claim 1, characterized in that said stimulus is presented orally.

3. A method as claimed in claim 2, characterized in that said stored data include stored representations of spoken sounds and said stimuli include requests to make one or more of said sounds to achieve random voice signature verification.

4. A method as claimed in claim 1 or 3, characterized in that said stored data include items of information within the personal knowledge of the customer and said stimuli include requests to provide verbal responses to questions

related to said items.

5. A method as claimed in claim 3, characterized in that voice recognition techniques are applied to extract response data from said verbal responses.

6. A method as claimed in claim 4, characterized in that said items of information are stored as digital representations of the customer's actual responses during set-up, and these are compared with said response data so as to match both content and voice-print in the same operation.

7. A customer authentication apparatus characterized in that it comprises:

a) a memory for storing digital data representing information items associated with each customer;

b) a selection unit for randomly selecting digital data associated with an information item on an iterative basis;

c) transducer means for presenting a stimulus related to said stored data to a customer wishing to access the service;

d) input means for accepting customer input in response to said stimulus and generating customer response data therefrom;

e) a comparator for comparing said customer response data with said stored data; and

f) validation means for validating said customer when said customer response data match said stored data within predefined limits.

8. A customer authentication apparatus as claimed in

claim 7, characterized in that said transducer means comprises a speaker and said input means comprises a microphone.

9. A customer authentication apparatus as claimed in claim 8, characterized in that some of said information items include representations of preselected sounds recorded by said customer.

10. A customer authentication apparatus as claimed in claim 9, characterized in that some of said information items include personal knowledge items.

11. A customer authentication apparatus as claimed in claim 8, characterized in that said transducer means and said input means are provided by a telephone connected to the rest of the apparatus by a telephone line.

12. A customer authentication apparatus as claimed in claim 11, further comprising a voice recognition unit for receiving customer input and generating response data therefrom.

13. A customer authentication apparatus as claimed in claim 7, characterized in that said memory stores digital representations of the customer's actual responses to knowledge-based queries, and said customer response data in the form of digital representations of the spoken responses are compared with said stored representations.

14. A method of authenticating a customer wishing to access a service, substantially as herein described, with

reference to the accompanying drawings.

15. A customer authentication apparatus substantially as herein described, with reference to or as shown in the accompanying drawings.

The Patent Office

17

Application No:	GB 9712528.0	**Examiner:**	Mike Davis
Claims searched:	1-15	**Date of search:**	31 July 1997

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): G4H (HTG)

Int Cl (Ed.6): G07F, G07C

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2112190 A	(OMRON)	1,7 at least
A	US 5365574	(HUNT ET AL)	-
X	US 5311594	(PENZIAS)	1,7 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.